

August 4, 2006

To: University Community
From: J. Robert Stanfield, Director Identity and Access Management Office

As more areas adopt PUID in place of Social Security Number as a unique identifier for Purdue University students, faculty, and staff, it is timely to remind the campus community that the PUID is classified as sensitive University data and should be handled accordingly.

The Purdue University Identifier (PUID) is a 10-digit number unique to each individual. The number is printed on a person's Purdue photo identification card. The PUID is designed to consistently establish an individual's identity for University business; replace the Social Security Number (SSN) as the primary University identifier; and have value only within the Purdue University system.

The data owner for the PUID is the Director of the Identity and Access Management Office. As this office has classified PUID as sensitive University data, the PUID should be handled according to Purdue's data handling guidelines for sensitive data. "Handling" information relates to when data is viewed, updated, or deleted. It also relates to the transfer of data from one location to another. It refers to both the electronic use and storage, and physical (i.e., paper-based) use and storage of the data.

Sensitive data handling requirements include the following:¹

- Documents containing PUID should be stored out of sight when not in use.
- Documents containing PUID should be disposed of in a manner such that they are physically destroyed beyond the ability to recover.
- The electronic storage of PUID on fixed media without access controls, but accessible via the web is not advised. If the data must be stored via this media, it must be encrypted.
- When transmitting PUID by fax, the receiving fax machine must have limited access such that only authorized persons can view the received fax. Otherwise, sender must first ensure that an authorized person will be present when the material is received via fax.
- When transmitting the PUID via wireless or cellular technology, the sender should be aware that wireless and/or cellular technologies are not very secure. Encryption suggested where applicable.
- When transmitting PUID by other electronic communications mechanisms (i.e., email, FTP, connections to administrative applications, etc.), encryption is suggested.

From Purdue Data Handling Requirements located at:

<http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>

Additional Resources:

PUID website: <http://www.purdue.edu/puid/Welcome.html>

Purdue's Data Classifications: <http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm>

Purdue's Data Handling Requirements: <http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>

SecurePurdue: <http://www.purdue.edu/securePurdue/>

¹ This list is not exhaustive; please see the data handling requirements for additional information.